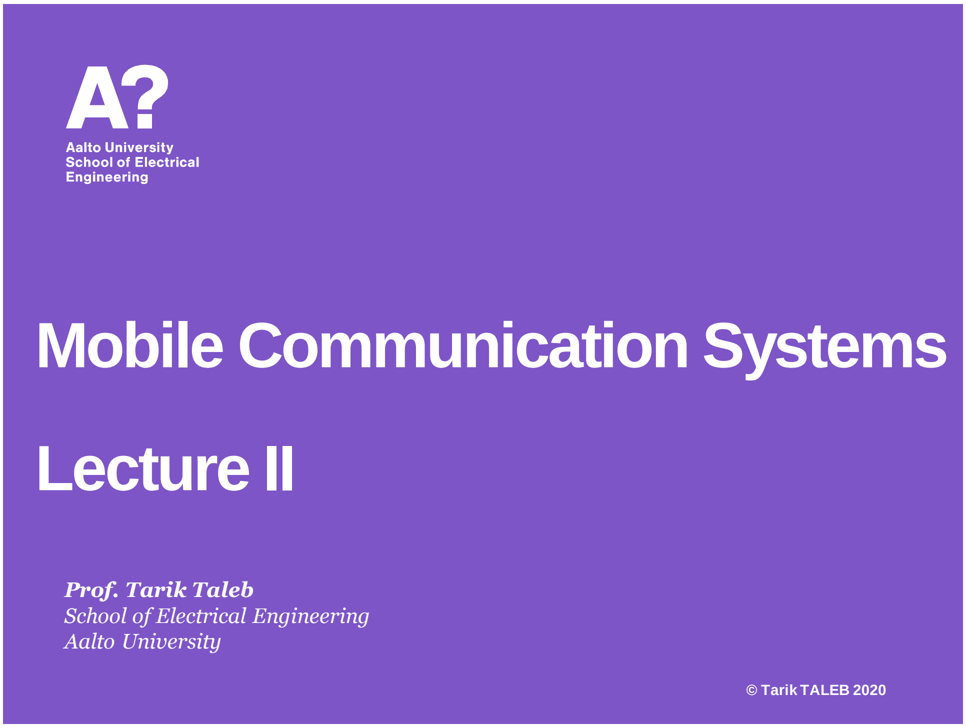


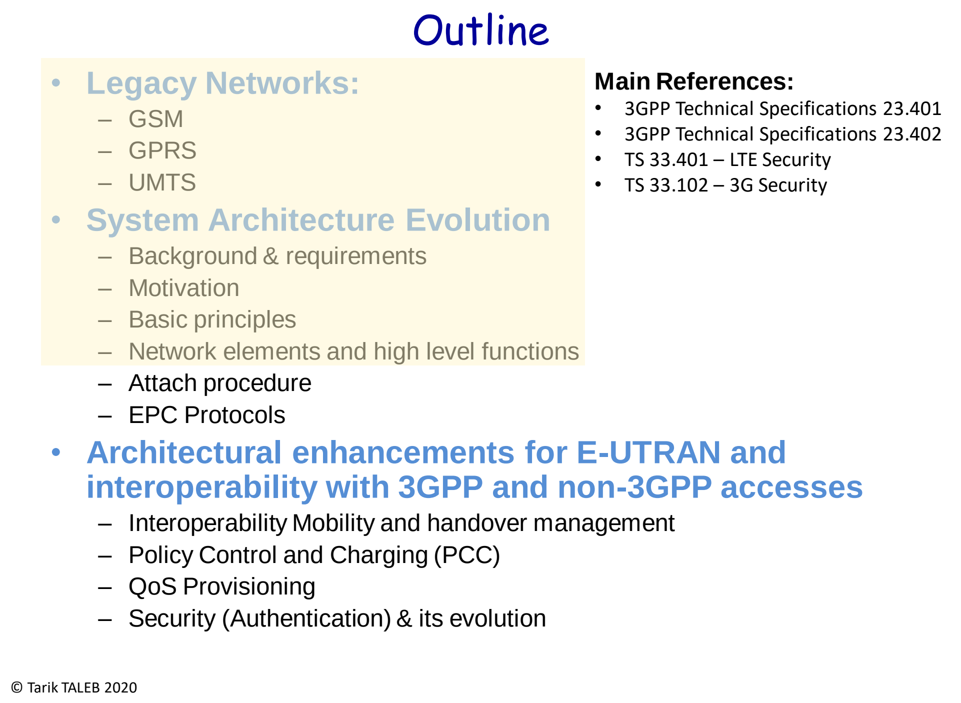
Aalto University
School of Electrical
Engineering

Mobile Communication Systems

Lecture II

Prof. Tarik Taleb
School of Electrical Engineering
Aalto University

44



Outline

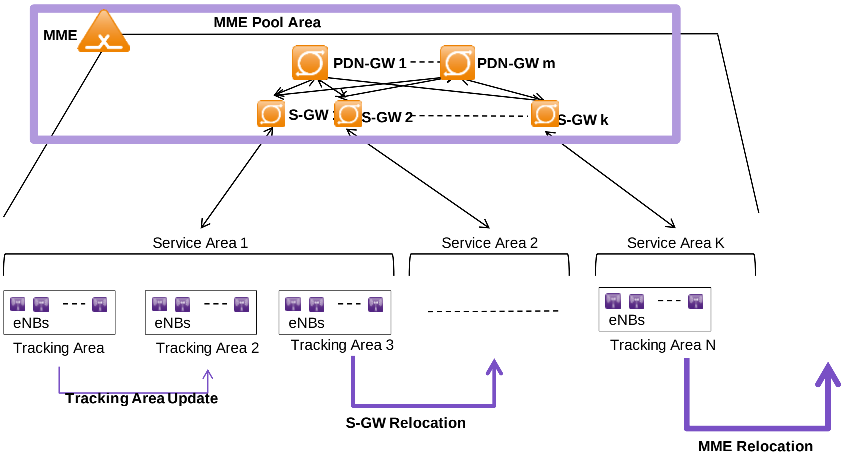
- Legacy Networks:
  - GSM
  - GPRS
  - UMTS
- System Architecture Evolution
  - Background & requirements
  - Motivation
  - Basic principles
  - Network elements and high level functions
  - Attach procedure
  - EPC Protocols
- **Architectural enhancements for E-UTRAN and interoperability with 3GPP and non-3GPP accesses**
  - Interoperability Mobility and handover management
  - Policy Control and Charging (PCC)
  - QoS Provisioning
  - Security (Authentication) & its evolution

Main References:

- 3GPP Technical Specifications 23.401
- 3GPP Technical Specifications 23.402
- TS 33.401 – LTE Security
- TS 33.102 – 3G Security

45

Tracking Areas, Service Areas, & MME Pool Areas

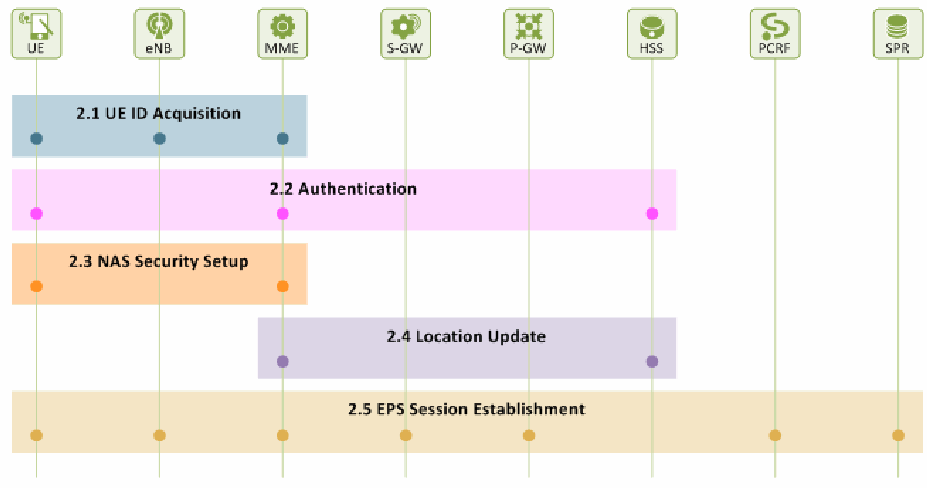


LTE UE Identifiers

- UE
  - IMEI or MEID - Mobile Equipment Identifier
    - Globally unique number identifying a physical piece of mobile station equipment
    - MEID allows hexadecimal digits while IMEI (Int'l Mobile Station Equipment Identity) allows only decimal digits
    - Only sent to MME (in NAS), not to eNB.
    - Sent only after NAS security is setup (i.e, encrypted and integrity protected).
- SIM (Subscriber Identity Module)
  - HD: Universal Integrated Circuit Card (UICC)
  - SW: USIM – Universal Subscriber Identity Module
    - IMSI
      - Seldom sent over the air (only during attach, if no other valid temporary ID is present in the UE).
      - Temporary identities used instead (S-TMSI, GUTI)
    - Brought, among other things, security improvements (e.g., mutual authentication, longer encryption keys, etc)

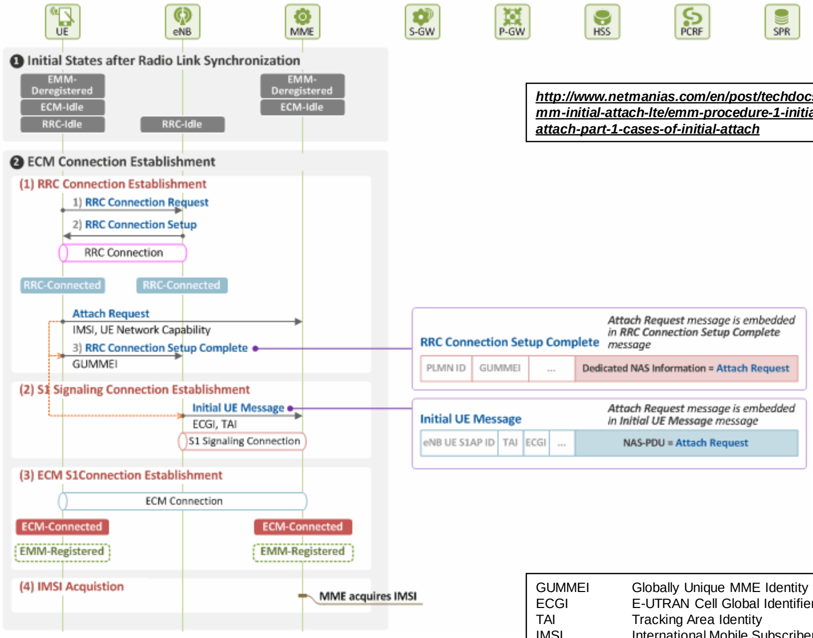
S-TMSI	System architecture evolution Temporary Mobile Subscriber Identity
GUTI	Globally Unique Temporary Identity

Initial Attach



http://www.netmanias.com/en/post/techdocs/6098/emm-initial-attach-lte/emm-procedure-1-initial-attach-part-1-cases-of-initial-attach

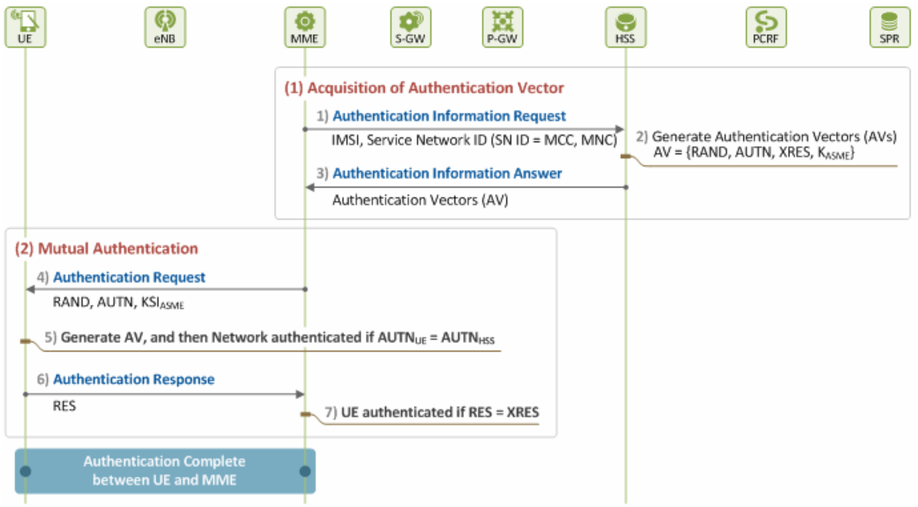
UE ID Acquisition


UE
eNB
MME
S-GW
P-GW
HSS
PCRF
SPR
❶ Initial States after Radio Link Synchronization
EMM-Deregistered
ECM-Idle
RRC-Idle
RRC-Idle
EMM-Deregistered
ECM-Idle
❷ ECM Connection Establishment
(1) RRC Connection Establishment
1) RRC Connection Request
2) RRC Connection Setup
RRC Connection
RRC-Connected
RRC-Connected
Attach Request
IMSI, UE Network Capability
3) RRC Connection Setup Complete
GUMMEI
(2) S1 Signaling Connection Establishment
Initial UE Message
ECGI, TAI
S1 Signaling Connection
(3) ECM S1Connection Establishment
ECM Connection
ECM-Connected
ECM-Connected
EMM-Registered
EMM-Registered
(4) IMSI Acquistion
MME acquires IMSI
RRC Connection Setup Complete
Attach Request message is embedded in RRC Connection Setup Complete message
PLMN ID
GUMMEI
...
Dedicated NAS Information = Attach Request
Initial UE Message
Attach Request message is embedded in Initial UE Message message
eNB UE S1AP ID
TAI
ECGI
...
NAS-PDU = Attach Request

http://www.netmanias.com/en/post/techdocs/6098/emm-initial-attach-lte/emm-procedure-1-initial-attach-part-1-cases-of-initial-attach

GUMMEI	Globally Unique MME Identity
ECGI	E-UTRAN Cell Global Identifier
TAI	Tracking Area Identity
IMSI	International Mobile Subscriber Identity

Authentication



(1) Acquisition of Authentication Vector

1) Authentication Information Request

IMSI, Service Network ID (SN ID = MCC, MNC)

2) Generate Authentication Vectors (AVs)
AV = {RAND, AUTN, XRES, K_{ASME}}

3) Authentication Information Answer

Authentication Vectors (AV)

(2) Mutual Authentication

4) Authentication Request

RAND, AUTN, KSI_{ASME}

5) Generate AV, and then Network authenticated if $AUTN_{UE}$ = $AUTN_{HSS}$

6) Authentication Response

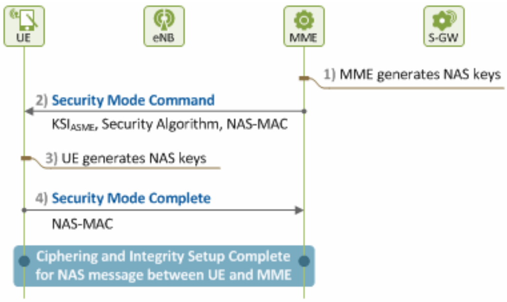
RES

7) UE authenticated if RES = XRES

Authentication Complete
between UE and MME

ASME	Access Security Management Entity (MME)
MCC	Mobile Country Code assigned by ITU, 3 digits
MNC	Mobile Network Code assigned by National Authority, 2~3 digits
AUTN	Authentication TokeN
KSI	Key Set Identifier

NAS Security Setup



1) MME generates NAS keys

2) Security Mode Command

KSI_{ASME}, Security Algorithm, NAS-MAC

3) UE generates NAS keys

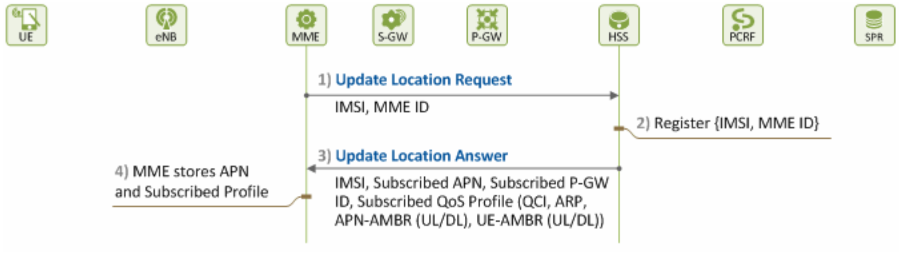
4) Security Mode Complete

NAS-MAC

Ciphering and Integrity Setup Complete
for NAS message between UE and MME

ASME	Access Security Management Entity (MME)
KSI	Key Set Identifier
NAS	Non-Access Stratum

Location Update



1) **Update Location Request**

IMSI, MME ID

2) Register {IMSI, MME ID}

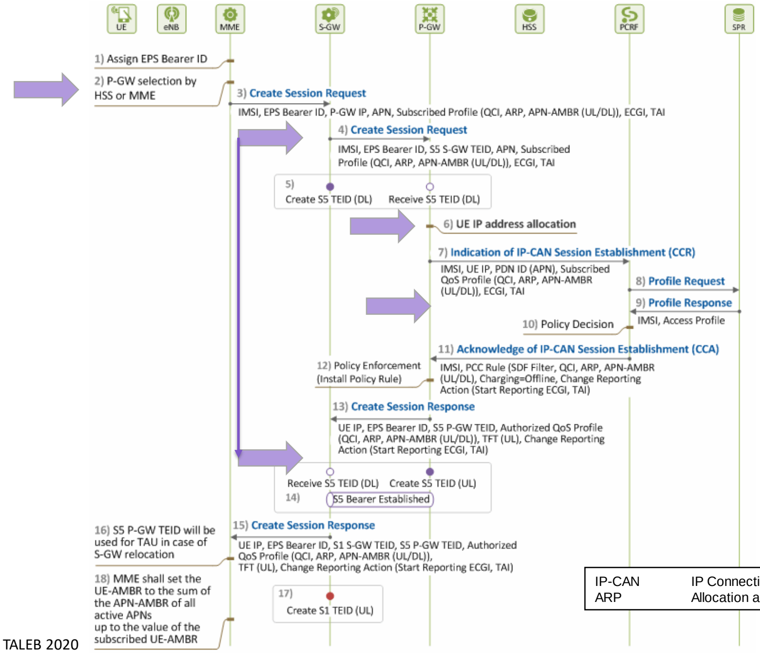
3) **Update Location Answer**

IMSI, Subscribed APN, Subscribed P-GW ID, Subscribed QoS Profile (QCI, ARP, APN-AMBR (UL/DL), UE-AMBR (UL/DL))

4) MME stores APN and Subscribed Profile

QCI: QoS Class Indicator
ARP: Allocation and Retention Priority
AMBR: Aggregate Maximum Bit Rates

EPS Session Management (1/2)



1) Assign EPS Bearer ID

2) P-GW selection by HSS or MME

3) **Create Session Request**

IMSI, EPS Bearer ID, P-GW IP, APN, Subscribed Profile (QCI, ARP, APN-AMBR (UL/DL)), ECGI, TAI

4) **Create Session Request**

IMSI, EPS Bearer ID, S5 S-GW TEID, APN, Subscribed Profile (QCI, ARP, APN-AMBR (UL/DL)), ECGI, TAI

5) Create S5 TEID (DL) Receive S5 TEID (DL)

6) UE IP address allocation

7) **Indication of IP-CAN Session Establishment (CCR)**

IMSI, UE IP, PDN ID (APN), Subscribed QoS Profile (QCI, ARP, APN-AMBR (UL/DL)), ECGI, TAI

8) **Profile Request**

9) **Profile Response**

IMSI, Access Profile

10) Policy Decision

11) **Acknowledge of IP-CAN Session Establishment (CCA)**

IMSI, PCC Rule (SDF Filter, QCI, ARP, APN-AMBR (UL/DL), Charging=Offline, Change Reporting Action (Start Reporting ECGI, TAI)

12) Policy Enforcement (Install Policy Rule)

13) **Create Session Response**

UE IP, EPS Bearer ID, S5 P-GW TEID, Authorized QoS Profile (QCI, ARP, APN-AMBR (UL/DL)), TFT (UL), Change Reporting Action (Start Reporting ECGI, TAI)

Receive S5 TEID (DL) Create S5 TEID (UL)

14) S5 Bearer Established

15) **Create Session Response**

UE IP, EPS Bearer ID, S1 S-GW TEID, S5 P-GW TEID, Authorized QoS Profile (QCI, ARP, APN-AMBR (UL/DL)), TFT (UL), Change Reporting Action (Start Reporting ECGI, TAI)

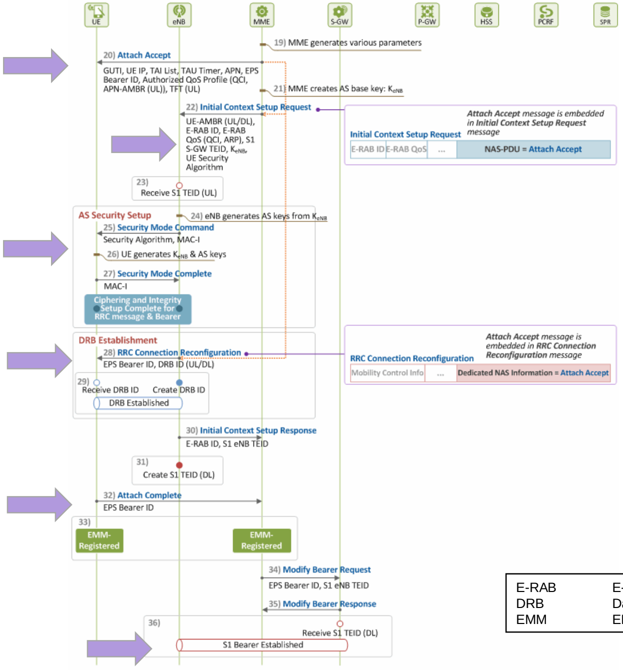
16) S5 P-GW TEID will be used for TAU in case of S-GW relocation

17) Create S1 TEID (UL)

18) MME shall set the UE-AMBR to the sum of the APN-AMBR of all active APNs up to the value of the subscribed UE-AMBR

IP-CAN	IP Connectivity Access Network
ARP	Allocation and Retention Priority

EPS Session Management (2/2)



19) MME generates various parameters

20) **Attach Accept**
GUTI, UE IP, TAI List, TAU Timer, APN, EPS Bearer ID, Authorized QoS Profile (QCI, APN-AMBR (UL)), TFT (UL)

21) MME creates AS base key: K_{eNB}

22) **Initial Context Setup Request**
UE-AMBR (UL/DL), E-RAB ID, E-RAB QoS (QCI, ARP), S1 S-GW TEID, K_{eNB}, UE Security Algorithm

Attach Accept message is embedded in Initial Context Setup Request message

Initial Context Setup Request

E-RAB ID	E-RAB QoS	...	NAS-PDU = Attach Accept

23) Receive S1 TEID (UL)

AS Security Setup

24) eNB generates AS keys from K_{eNB}

25) **Security Mode Command**
Security Algorithm, MAC-I

26) UE generates K_{eNB} & AS keys

27) **Security Mode Complete**
MAC-I

Ciphering and Integrity Setup Complete for RRC message & Bearer

DRB Establishment

28) **RRC Connection Reconfiguration**
EPS Bearer ID, DRB ID (UL/DL)

Attach Accept message is embedded in RRC Connection Reconfiguration message

RRC Connection Reconfiguration

Mobility Control Info	...	Dedicated NAS Information = Attach Accept

29) Receive DRB ID Create DRB ID
DRB Established

30) **Initial Context Setup Response**
E-RAB ID, S1 eNB TEID

31) Create S1 TEID (DL)

32) **Attach Complete**
EPS Bearer ID

33) EMM-Registered EMM-Registered

34) **Modify Bearer Request**
EPS Bearer ID, S1 eNB TEID

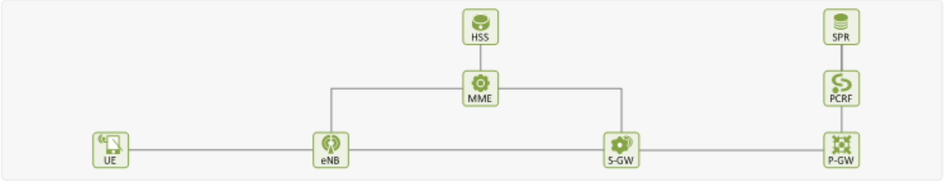
35) **Modify Bearer Response**

36) Receive S1 TEID (DL)
S1 Bearer Established

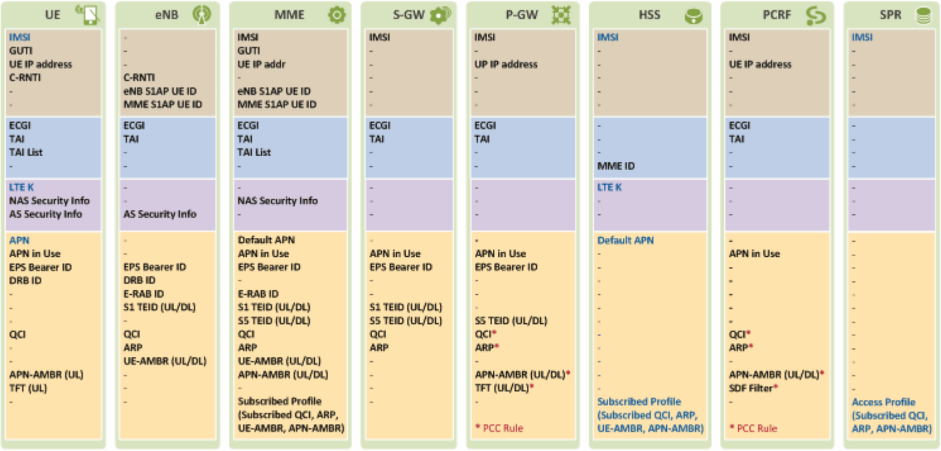
E-RAB	E-UTRAN Radio Access Bearer
DRB	Data Radio Bearer
EMM	EPS Mobility Management

Information Elements: Before Attach

UE	eNB	MME	S-GW	P-GW	HSS	PCRF	SPR
IMSI	-	-	-	-	IMSI	-	IMSI
-	-	-	-	-	-	-	-
LTE K	-	-	-	-	LTE K	-	-
APN -	- -	- -	- -	- -	Default APN Subscribed Profile (Subscribed QCI, ARP, UE-AMBR, APN-AMBR)	- -	- Access Profile (Subscribed QCI, ARP, APN-AMBR)



Information Elements: After Attach

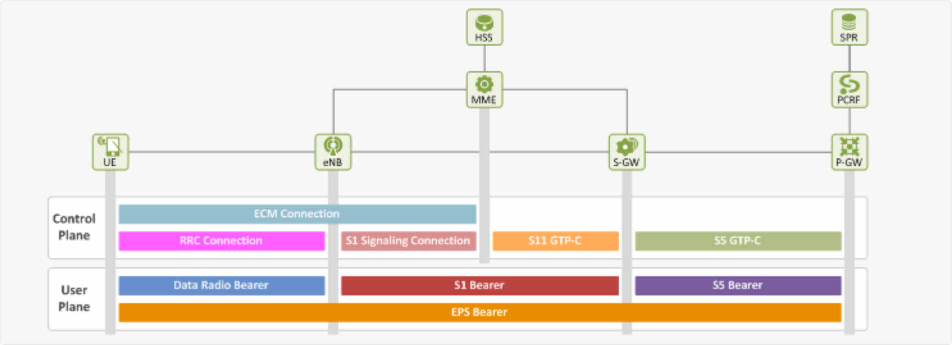


UE	eNB	MME	S-GW	P-GW	HSS	PCRF	SPR
IMSI	-	IMSI	IMSI	IMSI	IMSI	IMSI	IMSI
GUTI	-	GUTI	-	-	-	-	-
UE IP address	-	UE IP addr	-	UP IP address	-	UE IP address	-
C-RNTI	C-RNTI	-	-	-	-	-	-
-	eNB S1AP UE ID	eNB S1AP UE ID	-	-	-	-	-
-	MME S1AP UE ID	MME S1AP UE ID	-	-	-	-	-
ECGI	ECGI	ECGI	ECGI	ECGI	-	ECGI	-
TAI	TAI	TAI	TAI	TAI	-	TAI	-
TAI List	-	TAI List	-	-	-	-	-
-	-	-	-	-	MME ID	-	-
LTE K	-	-	-	-	LTE K	-	-
NAS Security Info	-	NAS Security Info	-	-	-	-	-
AS Security Info	AS Security Info	-	-	-	-	-	-
APN	-	Default APN	-	-	Default APN	-	-
APN in Use	-	APN in Use	APN in Use	APN in Use	-	APN in Use	-
EPS Bearer ID	EPS Bearer ID	EPS Bearer ID	EPS Bearer ID	EPS Bearer ID	-	-	-
DRB ID	DRB ID	-	-	-	-	-	-
-	E-RAB ID	E-RAB ID	-	-	-	-	-
-	S1 TEID (UL/DL)	S1 TEID (UL/DL)	S1 TEID (UL/DL)	-	-	-	-
-	-	S5 TEID (UL/DL)	S5 TEID (UL/DL)	S5 TEID (UL/DL)	-	-	-
QCI	QCI	QCI	QCI	QCI*	-	QCI*	-
-	ARP	ARP	ARP	ARP*	-	ARP*	-
-	UE-AMBR (UL/DL)	UE-AMBR (UL/DL)	-	-	-	-	-
APN-AMBR (UL)	-	APN-AMBR (UL/DL)	-	APN-AMBR (UL/DL)*	-	APN-AMBR (UL/DL)*	-
TFT (UL)	-	-	-	TFT (UL/DL)*	-	SDF Filter*	-
-	-	Subscribed Profile (Subscribed QCI, ARP, UE-AMBR, APN-AMBR)	-	-	Subscribed Profile (Subscribed QCI, ARP, UE-AMBR, APN-AMBR)	-	Access Profile (Subscribed QCI, ARP, APN-AMBR)
				* PCC Rule		* PCC Rule	

http://www.netmanias.com/en/post/techdocs/6098/emm-initial-attach-lte/emm-procedure-1-initial-attach-part-1-cases-of-initial-attach

57

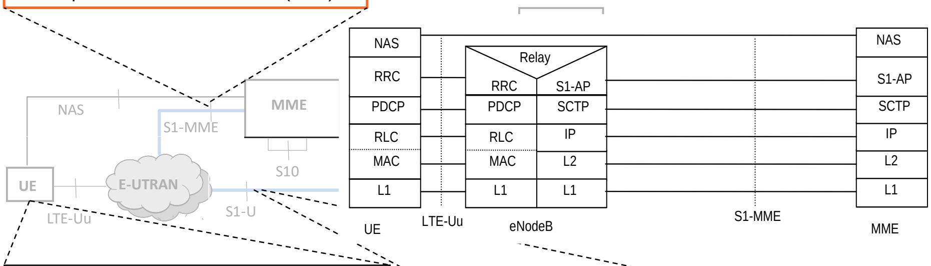
Some Nomenclature



58

Reference Points & Protocols

eNB-involved signaling: (over S1-AP)
Attachment, detachment, bearer establishment/modification, etc
Signaling transparent to eNB:
- on top of Non-Access Stratum (NAS)



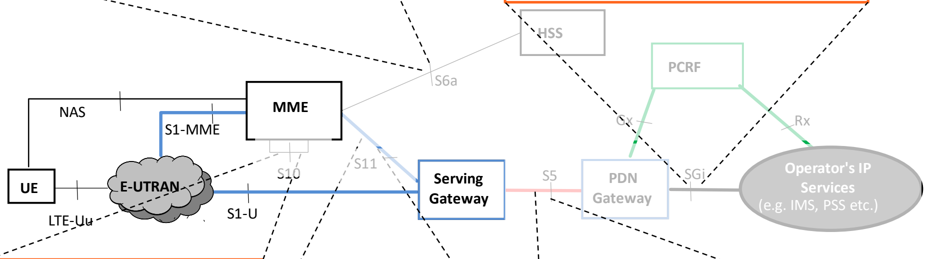
RRC – Radio Resource Control
PDCP – Packet Data Convergence Protocol
L2
L1

Encapsulation or tunneling of packets over GTP-U

Reference Points & Protocols

For exchange of UE subscription data (Diameter)

- IPv4/IPv6 for packet forwarding
- DHCP and RADIUS/DIAMETER for IP address and protocol configuration

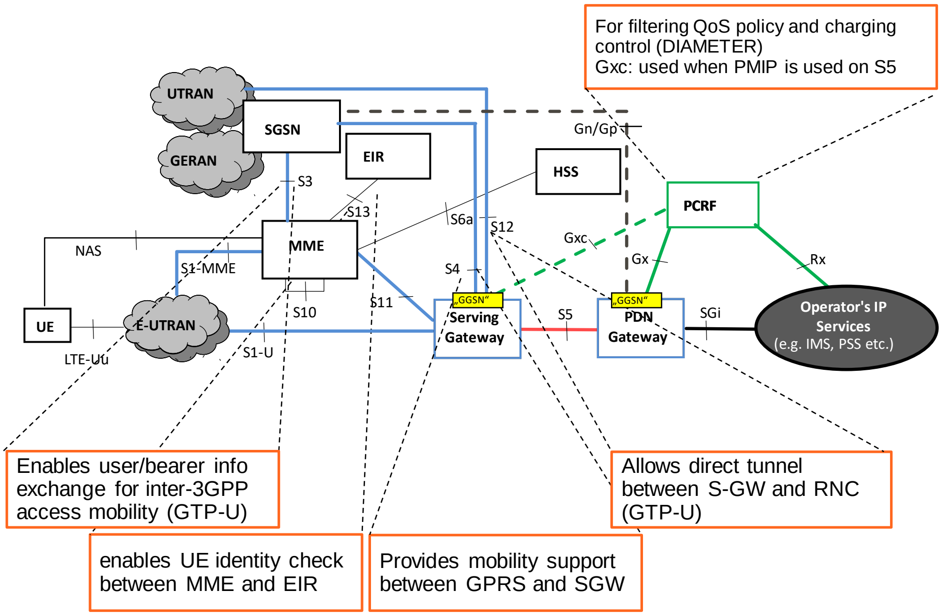


For MME relocation due to UE mobility or load balancing (GPT-C)

For controlling data bearer between eNB and SGW (GTP-C v2)

-Used when PGW and SGW are in HPLMN
- Based on either GTP or PMIP

Reference Points & Protocols



For filtering QoS policy and charging control (DIAMETER)
Gxc: used when PMIP is used on S5

Enables user/bearer info exchange for inter-3GPP access mobility (GTP-U)

Allows direct tunnel between S-GW and RNC (GTP-U)

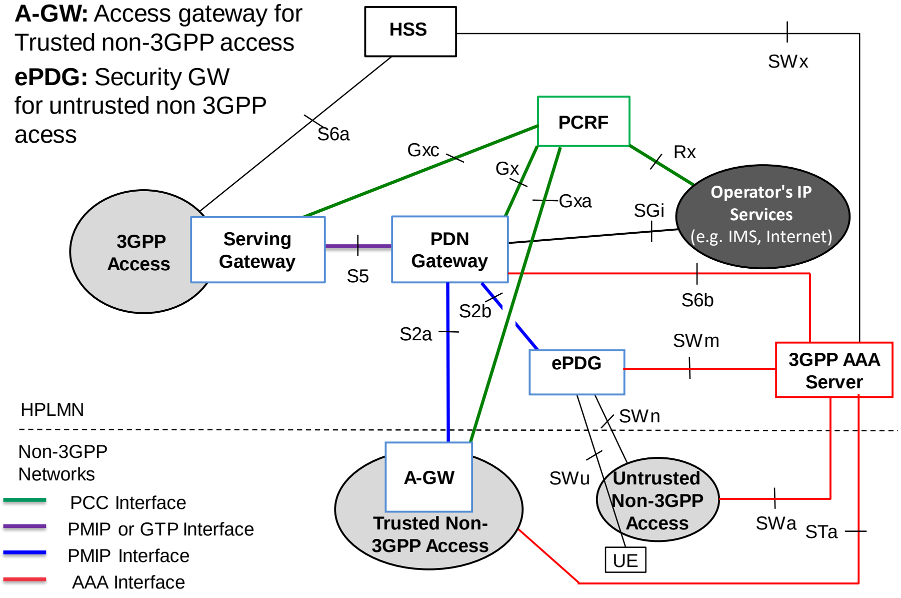
enables UE identity check between MME and EIR

Provides mobility support between GPRS and SGW

61

EPS – Overview

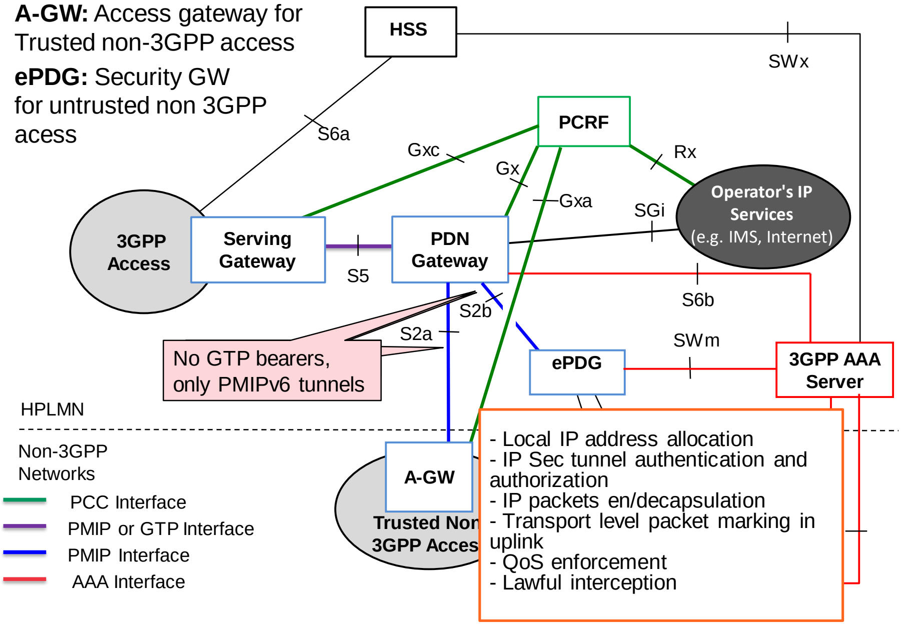
- **A-GW:** Access gateway for Trusted non-3GPP access
- **ePDG:** Security GW for untrusted non 3GPP acess



62

EPS for non-3GPP Accesses

- **A-GW:** Access gateway for Trusted non-3GPP access
- **ePDG:** Security GW for untrusted non 3GPP acess



No GTP bearers, only PMIPv6 tunnels

- Local IP address allocation
- IP Sec tunnel authentication and authorization
- IP packets en/decapsulation
- Transport level packet marking in uplink
- QoS enforcement
- Lawful interception

© Tarik TALEB 2020

A?
Aalto University
School of Electrical
Engineering

Inter Access System Handover

Service Continuity Support in EPC

- Two types of Service Continuity Support:
  - Mobility support within 3GPP networks (3GPP TS 23.401)
  - Mobility support between 3GPP and non-3GPP access systems (3GPP TS 23.402)
    - Network based mobility approach
      - Proxy Mobile IPv6 (PMIPv6)
    - Client based mobility approach
      - Dual-Stack Mobile IPv6 (DSMIPv6)

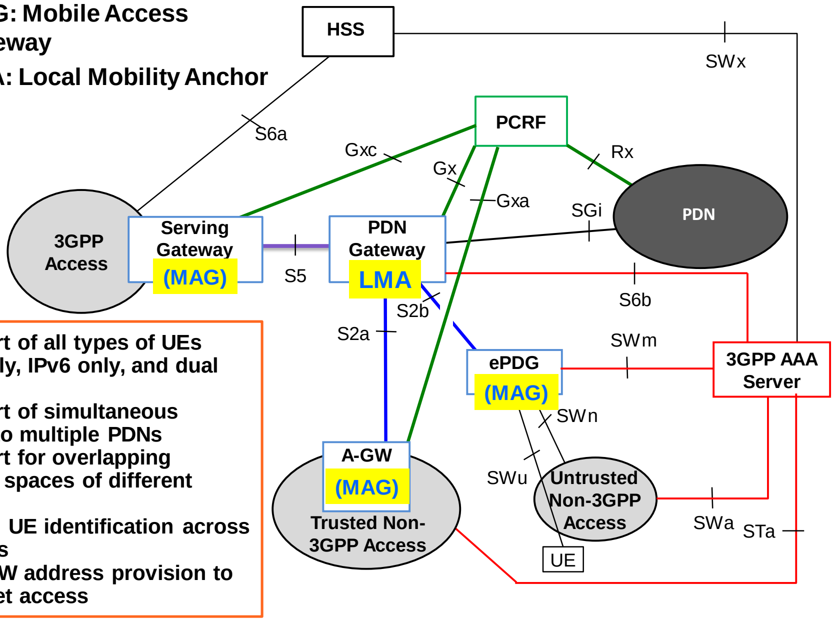
Which approach to adopt?

- **No perceivable service interruption**
- **Minimized handover delay**
- **Efficient use of wireless resources**
- **Wireless link could be bottleneck**
- **Minimized UE involvement**

65

PMIP's main Entities

- **MAG: Mobile Access Gateway**
- **LMA: Local Mobility Anchor**



- **Support of all types of UEs (IPv4 only, IPv6 only, and dual stack)**
- **Support of simultaneous access to multiple PDNs**
- **Support for overlapping address spaces of different PDNs**
- **Unique UE identification across accesses**
- **PDN GW address provision to the target access**

66

Inter-Access System Mobility Flows

- **Non-optimized handover flows**
  - Source network not being involved
  - Suitable for dual radio capable terminals
- **Optimized handover flows**
  - Involving source network
  - Suitable for single radio terminals
  - Initially defined for mobility between CDMA2000 eHRPD and E-UTRAN

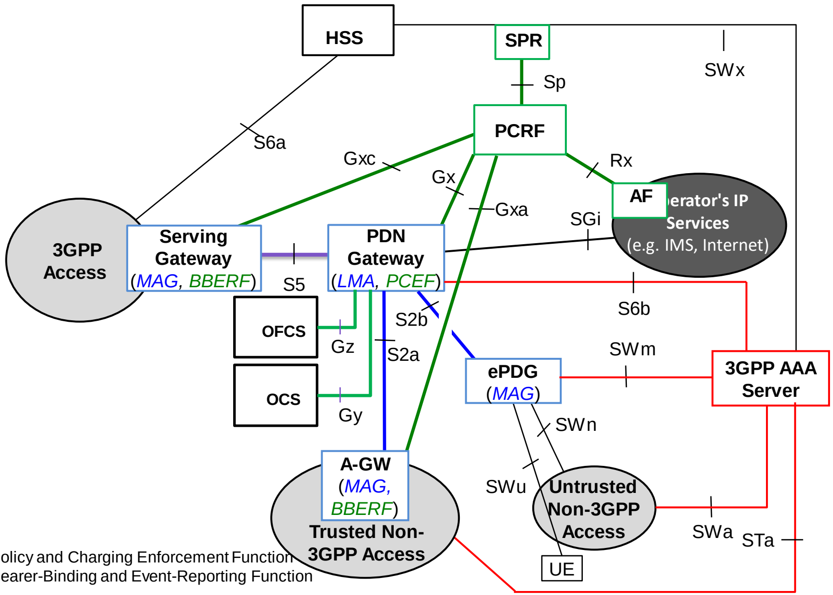
Aalto University
School of Electrical
Engineering

Policy and Charging Control

PCC Evolution

- Background:
  - **Service-Based Local Policy (SBLP)** for resource reservation and access control within IMS
    - Bearer-level QoS control
    - **Service level access control**
  - Further enhancement of SBLP in Rel. 6
  - Introduction of **Flow-Based Charging (FBC)** in Rel. 6
    - ***Per-service charging:* offline and online models**
    - **Per-service/content access control**
  - Similarities between SBLP and FBC
    - Centralized
    - Same anchor points: AF and GGSN
  - Merging SBLP and FBC in Rel. 7 ➔ PCC
  - Continuous enhancements of PCC in Rel. 8 and beyond
- Objectives:
  - Support of IP services' QoS
  - Charging subscribers for used resources

PCC Interfaces and Protocols



HSS

SPR

Sp

SWx

PCRF

S6a

Gxc

Gx

Rx

Gxa

AF

SGi

Operator's IP Services (e.g. IMS, Internet)

3GPP Access

Serving Gateway (MAG, BBERF)

S5

PDN Gateway (LMA, PCEF)

S6b

OFCS

Gz

S2b

S2a

SWm

OCS

Gy

ePDG (MAG)

3GPP AAA Server

SWn

A-GW (MAG, BBERF)

Trusted Non-3GPP Access

SWu

Untrusted Non-3GPP Access

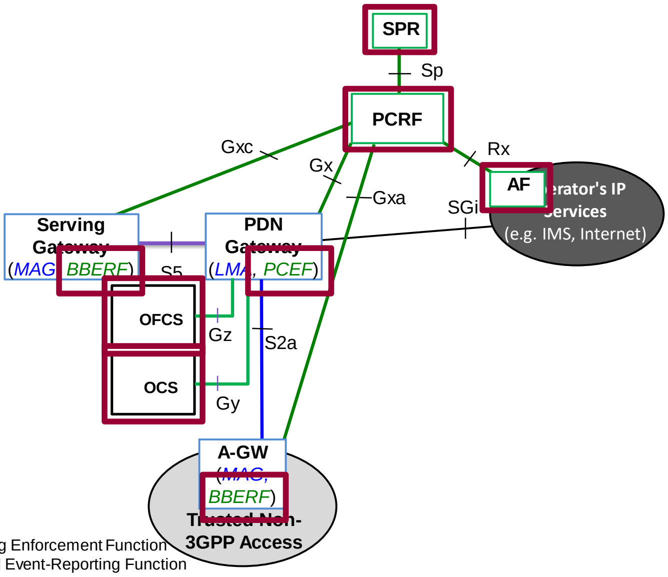
UE

SWa

STa

PCEF	Policy and Charging Enforcement Function
BBERF	Bearer-Binding and Event-Reporting Function
OCS	Online Charging System
OFCS	OFfline Charging System
SPR	Subscription Profile Repository

PCC Key Components



PCEF	Policy and Charging Enforcement Function
BBERF	Bearer-Binding and Event-Reporting Function
OCS	Online Charging System
OFCS	OFfline Charging System
SPR	Subscription Profile Repository

Subset of Available Parameters in the PCC Rule

Type of element	PCC rule element	Comment
Rule identification	Rule identifier	Used between PCRF and PCEF for referencing PCC rules
Items related to service data flow detection in PCEF	Service data flow template	List of packet filters for the detection of the service data flow
	Precedence	Determines the order in which the service data flow templates are applied at PCEF
Items related to policy control (i. e. gating and QoS control)	Gate status	Indicates whether a SDF may pass (gate open) or shall be discarded (gate closed)
	QoS class identifier (QCI)	Identifier that represents the packet forwarding behavior of a flow
	UL and DL maximum bit rates	The maximum bitrates authorized for the service data flow
	UL and DL guaranteed bit rates	The guaranteed bitrates authorized for the service data flow
Items related to charging control	Charging key	The charging system uses the charging key to determine the tariff to apply for the service data flow
	Charging method	Indicates the required charging method for the PCC rule. Values: online, offline, or no charging
	Measurement method	Indicates whether the SDF data volume, duration, combined volume/duration or event shall be measured

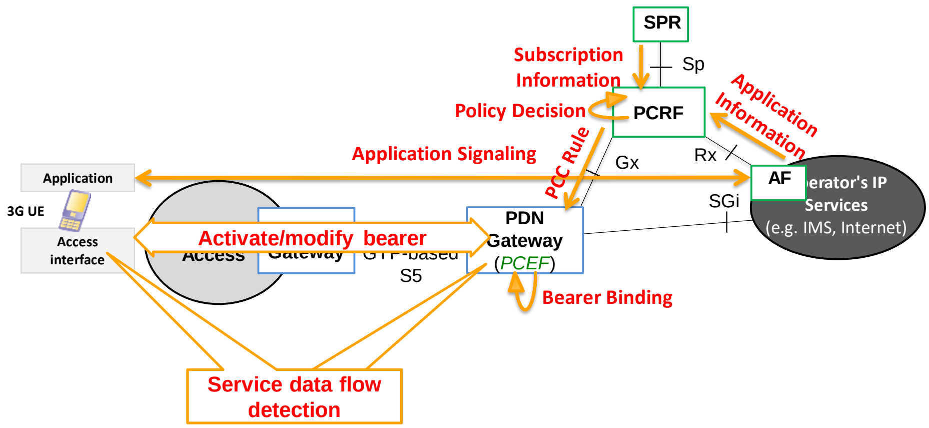
PCC Architecture Types

- **On-Path Model**:
  - without BBERF in access gateway (in case of GTP)
  - QoS/bearer signaling (using GTP) on the same path as user plane
- **Off-Path Model**:
  - with BBERF in access gateway (in case of PMIP)
  - QoS signaling (using Gxa/Gxc) on a path different from that of user plane

Basic PCC Concepts

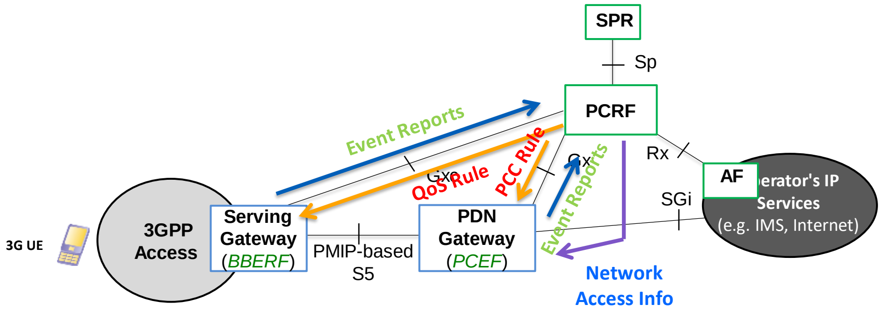
- **Gating Control**:
  - Blocks or allows Service Data Flows (e.g. based on indicators from AF)
- **QoS Control**:
  - Provides PCEF with authorized QoS class and bit rates for IP flows
- **Charging Control**:
  - Online charging
  - Offline charging
  - NO charging

Use Case: "On-Path" Model



PCEF	Policy and Charging Enforcement Function
BBERF	Bearer-Binding and Event-Reporting Function
OCS	Online Charging System
OFCS	OFfline Charging System
SPR	Subscription Profile Repository

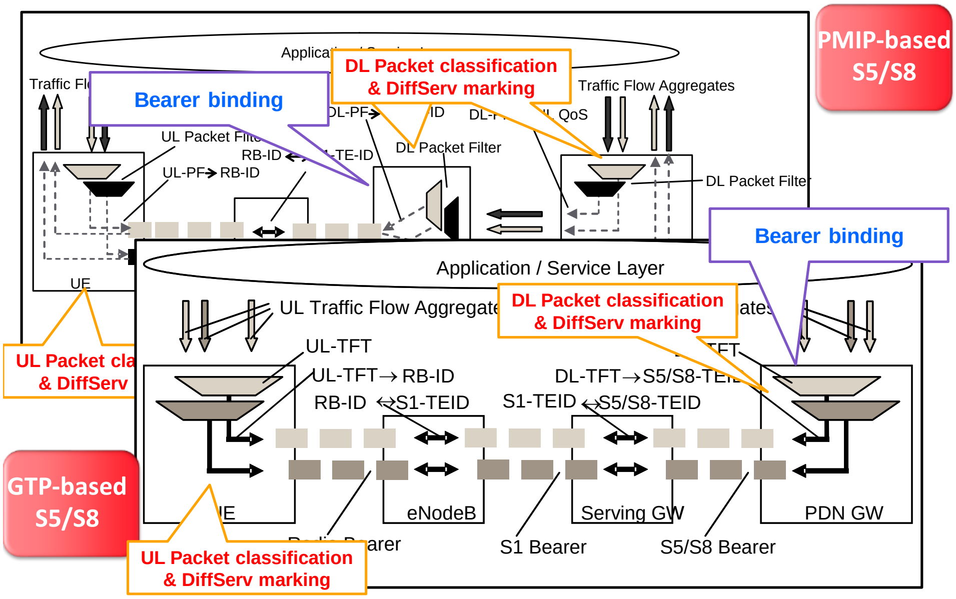
Use Case: "Off-Path" Model



QoS and Policy Control

- QoS is enforced at the granularity of EPS bearers
  - UE ←→ PDN GW (for GTP-based EPC)
  - UE ←→ Serving GW (for PMIP-based EPC)
- An EPS bearer uniquely identifies traffic flows
  - Default Bearer
  - Dedicated Bearers (for flows requiring special QoS treatment)
- EPS bearer QoS profile:
  - QCI: QoS Class Indicator
  - ARP: Allocation and Retention Priority
  - GBR: Guaranteed Bit Rate

QoS over IP Transport



PMIP-based S5/S8

Bearer binding

DL Packet classification & DiffServ marking

UL Packet cla & DiffServ

Bearer binding

DL Packet classification & DiffServ marking

GTP-based S5/S8

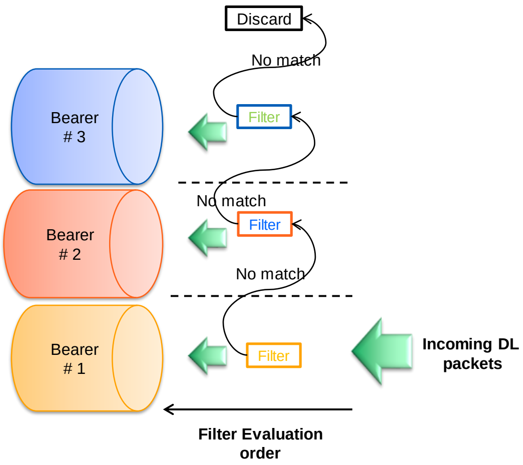
UL Packet classification & DiffServ marking

Bearer Binding

- Mapping a PCC rule to a corresponding QoS bearer
- Performed by Bearer-Binding Function (BBF)
  - in PCEF for on-path model
  - in BBERF for off-path model
- Upon receiving a new or modified PCC rule, BBF first verifies whether an existing bearer can be used
  - If yes, BBF modifies bearer by adjusting bearer's bit rates
  - If not, BBF sets up a new bearer

79

Service Data Flow Detection



80

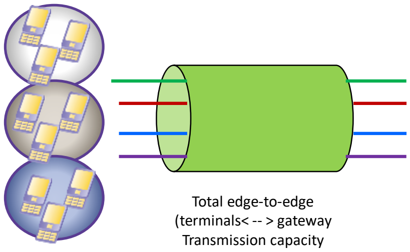
Aalto University
School of Electrical
Engineering

QoS Control in EPS (using PCC)

Service/Subscriber Differentiation

Subscriber differentiation

- Business vs. standard
- Post- vs. pre-paid roamers
- Privileged (e.g. police)
- Flat rate abusers



Service differentiation

- Public internet
- Corporate (VPN)
- Premium content
- P2P file sharing
- Video streaming
- IMS voice
- Mobile-TV

EPS QoS Concept

- Bearer types
  - GBR vs. non-GBR bearers
  - Default vs. Dedicated Bearers
- QoS Parameters
  - QCI: QoS Class Indicator
    - 1 to 9:
    - QCI = 1 ➔ Resource Type = GBR, Priority = 2, Packet Delay Budget = 100ms, Packet Error Loss Rate = 10-2 , Example Service = Voice
    - QCI = 9 ➔ Resource Type = Non-GBR, Priority = 9, Packet Delay Budget = 300ms, Packet Error Loss Rate = 10-6, Example Service = Internet
  - ARP: Allocation and Retention Priority
    - In 4G, ARP priority level (PL) values range from 1 through 15, where 1 corresponds to the highest priority and 15 corresponds to the lowest priority.
    - Used to accept or reject a bearer request, when resources are limited
  - MBR: Maximum Bit Rates
  - GBR: Guaranteed Bit Rate
- QoS Mechanisms
  - Control Plane Signaling Procedures
  - User Plane Functions
  - Packet-Flow-Level Functions
  - Bearer-Level Functions
  - DSCP-Level Functions

DSCP	Differentiated Service Code Point

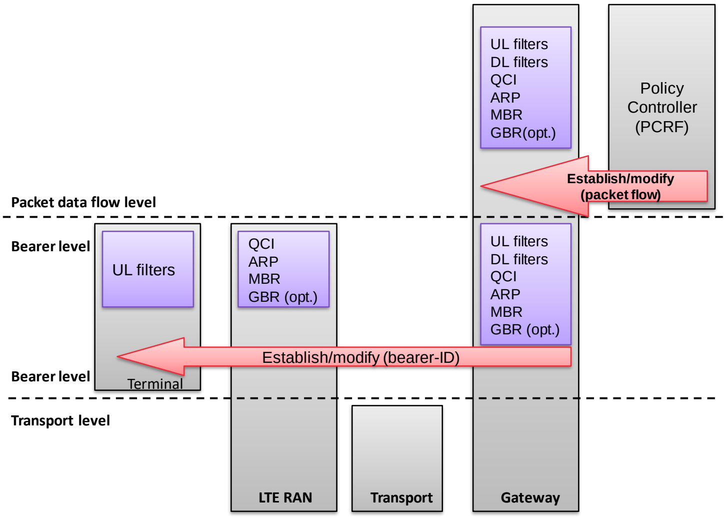
Bearer Types

- **Guaranteed bit-rate (GBR) bearer**:
  - Established “on demand”
  - No congestion due packet losses
  - Suitable for services tolerating “service blocking over service dropping”
- **Non-GBR bearer:**
  - No resources blocked
  - May experience packet losses
- **Default bearer:**
  - One default bearer per terminal IP address
  - For basic connectivity.
  - non-GBR
  - QoS level depending on subscription data
  - Not associated with any specific packet filter
- **Dedicated bearer:**
  - Either non-GBR or GBR
  - Packet flows mapping onto dedicated bearers based on operator policies

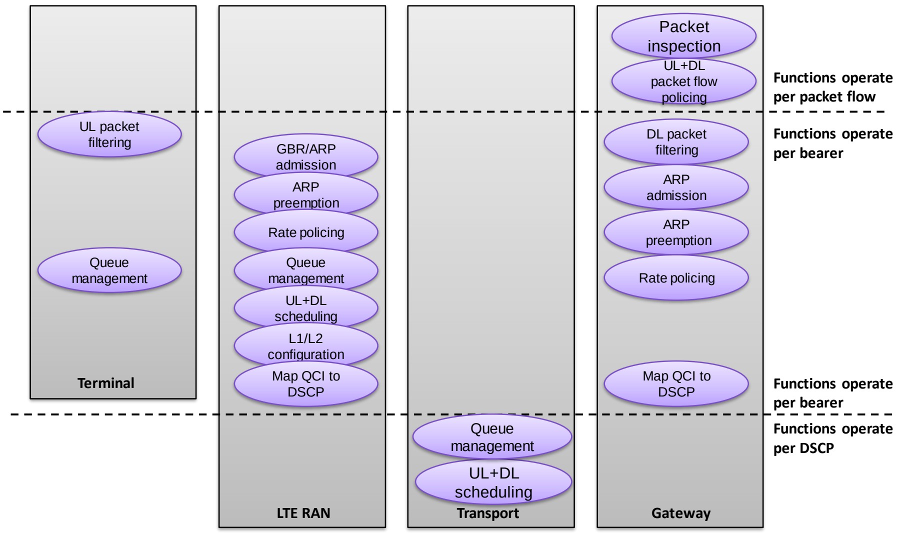
QoS Parameters

- **QoS Class Identifier (QCI):**
  - a reference to node-specific pre-configured parameters that control packet-forwarding treatment at the user plane
- **Allocation and Retention Priority (ARP)**
  - Specifies control plane treatment for bearers
- **Maximum Bit Rate (MBR)**
  - Bit rate traffic on a bearer may not exceed
- **Guaranteed Bit Rate (GBR)**
  - Bit rate that the network guarantees for a bearer
- **Aggregate Maximum Bit Rate (AMBR)**:
  - Limit to the total amount of bit rates consumed by a single subscriber (excluding GBR bearers)
    - **UL/DL APN-AMBR**: defined per subscriber and APN and known only to the gateway
    - **UL/DL Terminal-AMBR**: defined per subscriber and known by both the gateway and RAN

QoS Mechanisms - Control Plane Signaling Procedures -

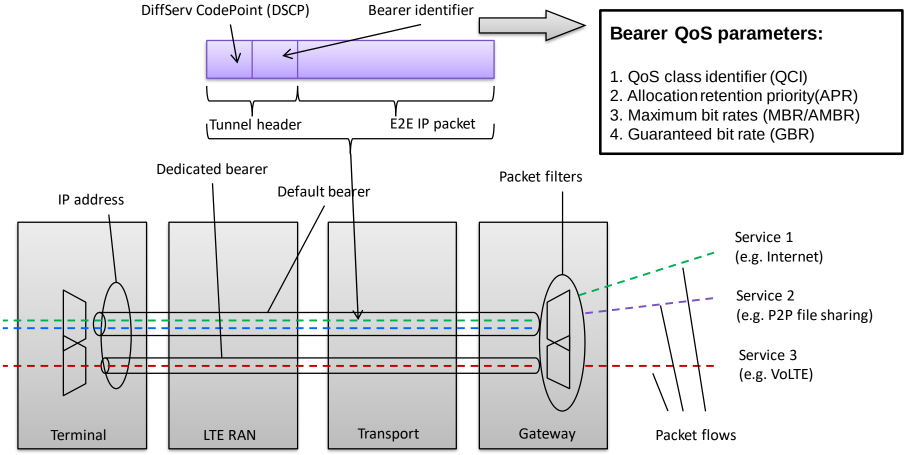


QoS Mechanisms - User-Plane Functions -



DSCP Differentiated Service Code Point

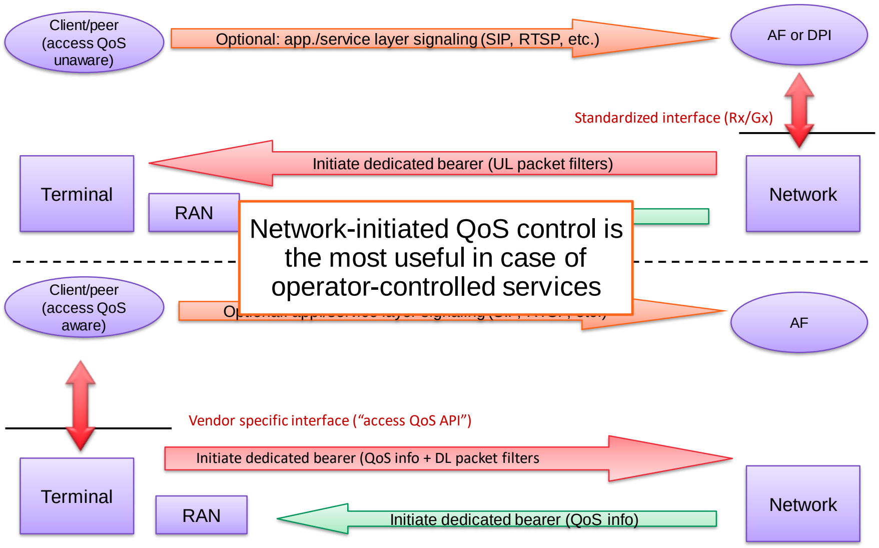
DSCP vs QCI



Bearer QoS parameters:

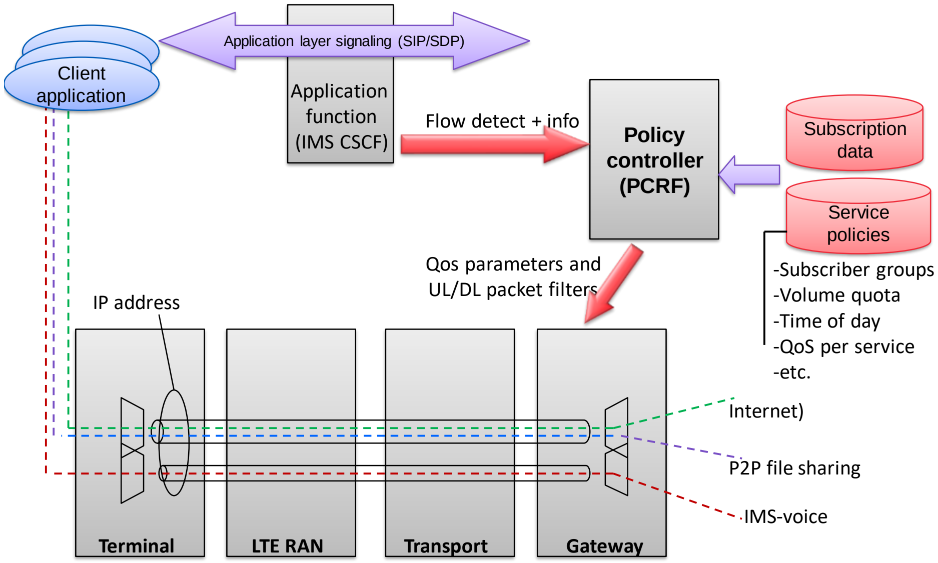
1. QoS class identifier (QCI)
2. Allocation retention priority(APR)
3. Maximum bit rates (MBR/AMBR)
4. Guaranteed bit rate (GBR)

Dedicated Bearer Establishment: Network- vs. Terminal-initiated


Client/peer (access QoS unaware)
Optional: app./service layer signaling (SIP, RTSP, etc.)
AF or DPI
Standardized interface (Rx/Gx)
Terminal
Initiate dedicated bearer (UL packet filters)
Network
RAN
Client/peer (access QoS aware)
Op
AF
Vendor specific interface ("access QoS API")
Initiate dedicated bearer (QoS info + DL packet filters
Terminal
RAN
Initiate dedicated bearer (QoS info)
Network

Network-initiated QoS control is the most useful in case of operator-controlled services

Summing Up All: E2E Use Case



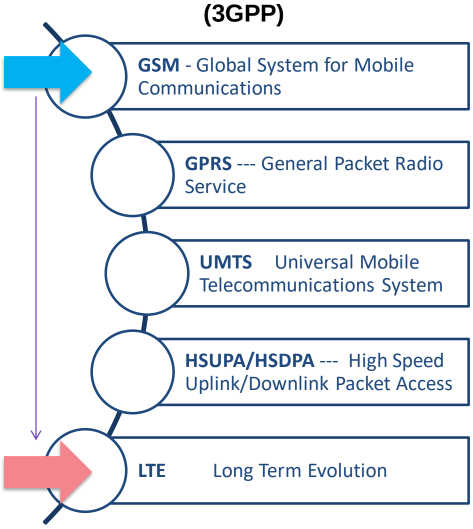
A?
Aalto University
School of Electrical
Engineering

Security: Authentication

91

Authentication Evolution from GSM to LTE

3^{rd} Generation Partnership Program (3GPP)



GSM - Global System for Mobile Communications

GPRS --- General Packet Radio Service

UMTS Universal Mobile Telecommunications System

HSUPA/HSDPA --- High Speed Uplink/Downlink Packet Access

LTE Long Term Evolution

92

Authentication in brief

- Authentication
  - Establishing or confirming something (or someone) as authentic
  - **Mutual authentication**, means network authenticates the user and the user authenticates the network

- An important security function
  - Authorization
  - Integrity protection
  - Replay protection
  - Privacy
  - etc

TS 33.401 – LTE Security
TS 33.102 – 3G Security

User Authentication

- PIN – Personal Identification Number
- PUK – PIN Unlocked Key – or PUC (Personal Unlock Code)

LTE UE Identifiers

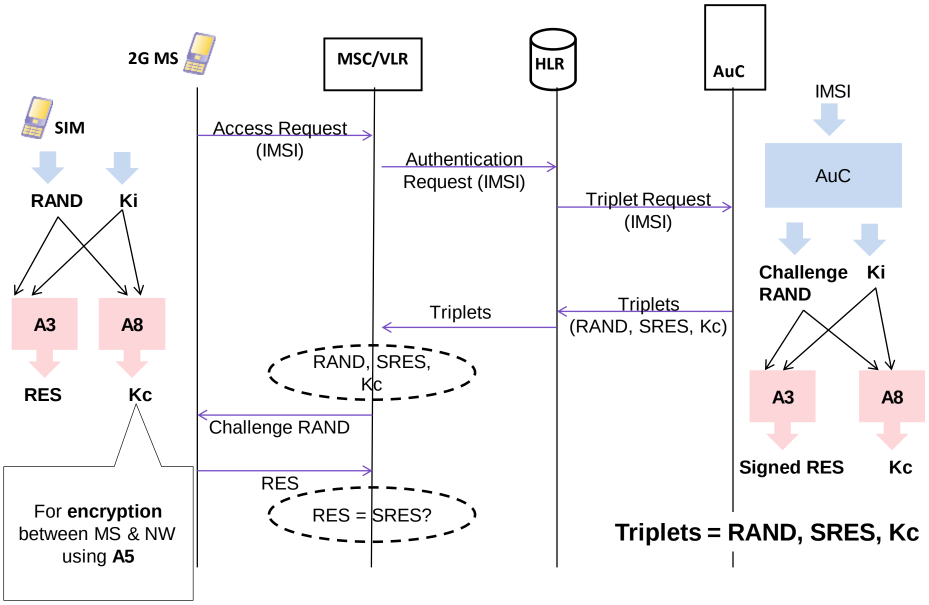
- UE
  - IMEI or MEID - Mobile Equipment Identifier
    - Globally unique number identifying a physical piece of mobile station equipment
    - MEID allows hexadecimal digits while IMEI (Int’l Mobile Station Equipment Identity) allows only decimal digits
    - Only sent to MME (in NAS), not to eNB.
    - Sent only after NAS security is setup (i.e, encrypted and integrity protected).
- SIM (Subscriber Identity Module)
  - HD: Universal Integrated Circuit Card (UICC)
  - SW: USIM – Universal Subscriber Identity Module
    - IMSI
      - Seldom sent over the air (only during attach, if no other valid temporary ID is present in the UE).
      - Temporary identities used instead (S-TMSI, GUTI)
    - Brought, among other things, security improvements (e.g., mutual authentication, longer encryption keys, etc)

S-TMSI	System architecture evolution Temporary Mobile Subscriber Identity
GUTI	Globally Unique Temporary Identity

GSM Mobile Station

- Mobile Equipment (ME)
  - Physical mobile device
  - Identifiers
    - IMEI – International Mobile Equipment Identity
- Subscriber Identity Module (SIM)
  - Smart Card containing keys, identifiers and algorithms
  - Identifiers
    - **K_i** – Subscriber Authentication Key
    - **IMSI** – International Mobile Subscriber Identity
    - **TMSI** – Temporary Mobile Subscriber Identity
    - **MSISDN** – Mobile Station International Service Digital Network
    - Authentication Algorithms (**A3, A8**)
    - Stream Ciphering/Encryption Algorithm (**A5**)
    - **PIN** – Personal Identity Number protecting a SIM
    - Others

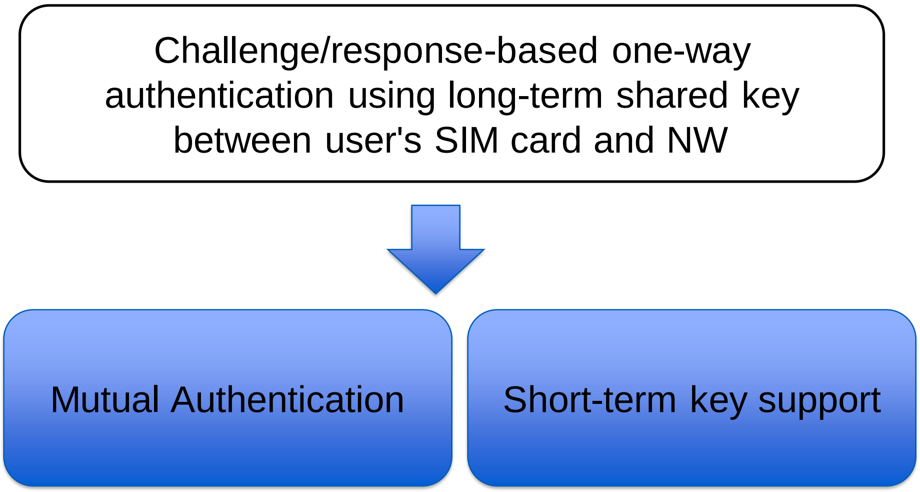
Authentication Flow in GSM



Triplets = RAND, SRES, Kc

© Tarik TALEB 2020

GSM Authentication Principle

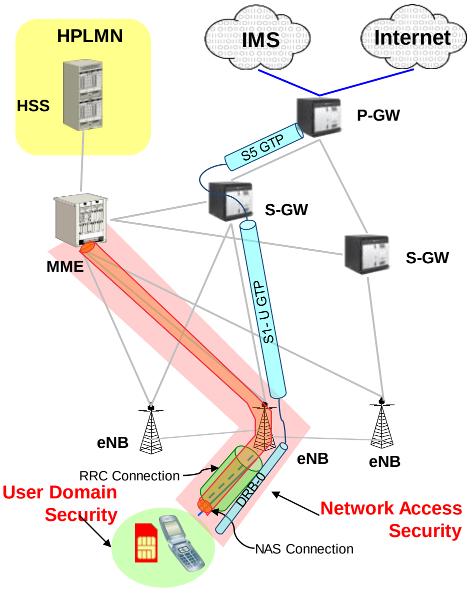

Challenge/response-based one-way authentication using long-term shared key between user's SIM card and NW

Mutual Authentication

Short-term key support

© Tarik TALEB 2020

Overall Architecture of Evolved Packet System

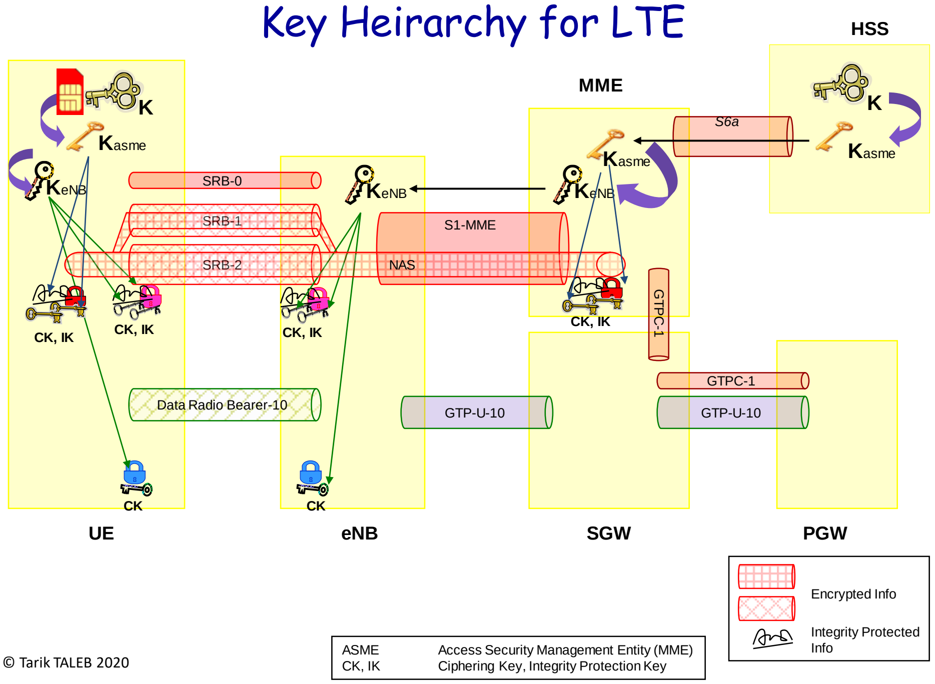


LTE User Equipment

- UE
  - IMEI or MEID - Mobile Equipment Identifier
    - Globally unique number identifying a physical piece of mobile station equipment
    - MEID allows hexadecimal digits while IMEI (Int’l Mobile Station Equipment Identity) allows only decimal digits
- SIM
  - HD: Universal Integrated Circuit Card (UICC)
  - SW: USIM – Universal Subscriber Identity Module
    - IMSI
      - Seldom sent over the air (only during attach, if no other valid temporary ID is present in the UE).
      - Temporary identities used instead (S-TMSI, GUTI)
    - Brought, among other things, security improvements (e.g., mutual authentication, longer encryption keys, etc)

S-TMSI	System architecture evolution Temporary Mobile Subscriber Identity
GUTI	Globally Unique Temporary Identity

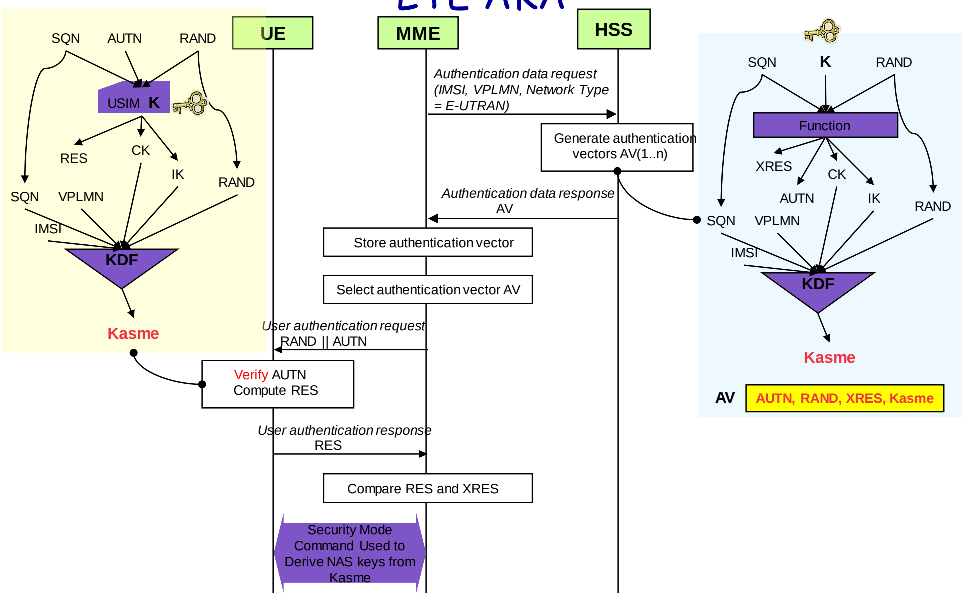
Key Heirarchy for LTE



ASME	Access Security Management Entity (MME)
CK, IK	Ciphering Key, Integrity Protection Key

101

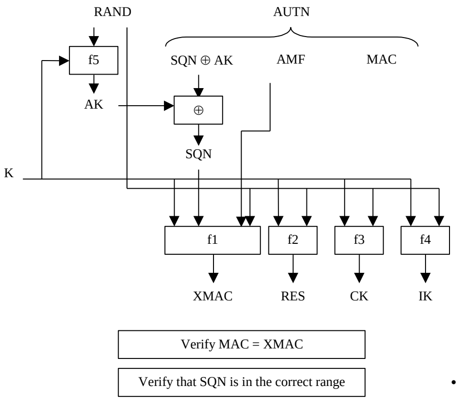
LTE AKA


UE
MME
HSS
SQN
AUTN
RAND
USIM K
RES
CK
IK
RAND
SQN
VPLMN
IMSI
KDF
Kasme
Authentication data request (IMSI, VPLMN, Network Type = E-UTRAN)
Generate authentication vectors AV(1..n)
Authentication data response AV
Store authentication vector
Select authentication vector AV
User authentication request RAND || AUTN
Verify AUTN Compute RES
User authentication response RES
Compare RES and XRES
Security Mode Command Used to Derive NAS keys from Kasme
SQN
K
RAND
Function
XRES
CK
AUTN
IK
RAND
SQN
VPLMN
IMSI
KDF
Kasme
AV
AUTN, RAND, XRES, Kasme

AUTN	Authentication TokeN
GUTI	Globally Unique Temporary Identity
KSI	Key Set Identifier

102

User authentication function in the USIM

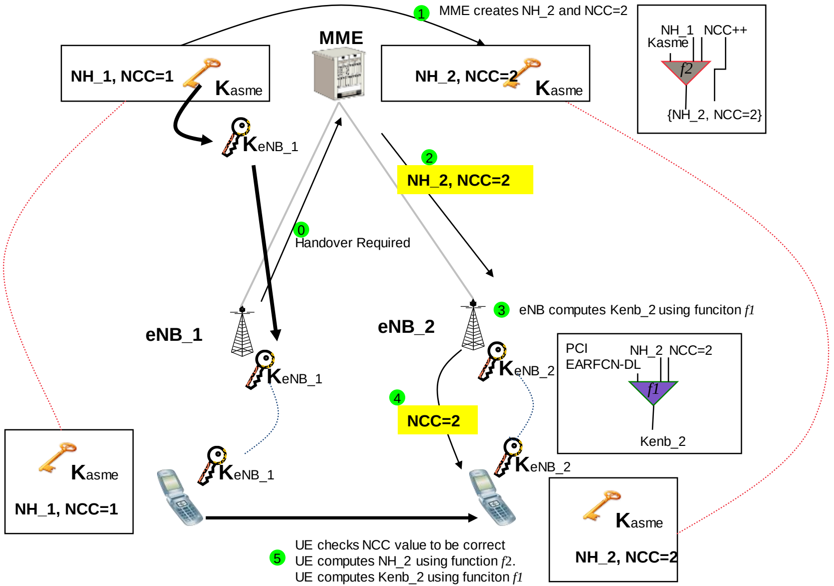


- USIM keeps track of last SQN received, SQNms
- USIM only accepts a sequence number from HSS if |SQN – SQNms | < Δ

AUTN	Authentication TokeN
AMF	Authentication management field
SQN	Sequence Number
AK	Anonymity Key
MAC	Message Authentication Code

103

Kenb Key Derivation at S1 Handover

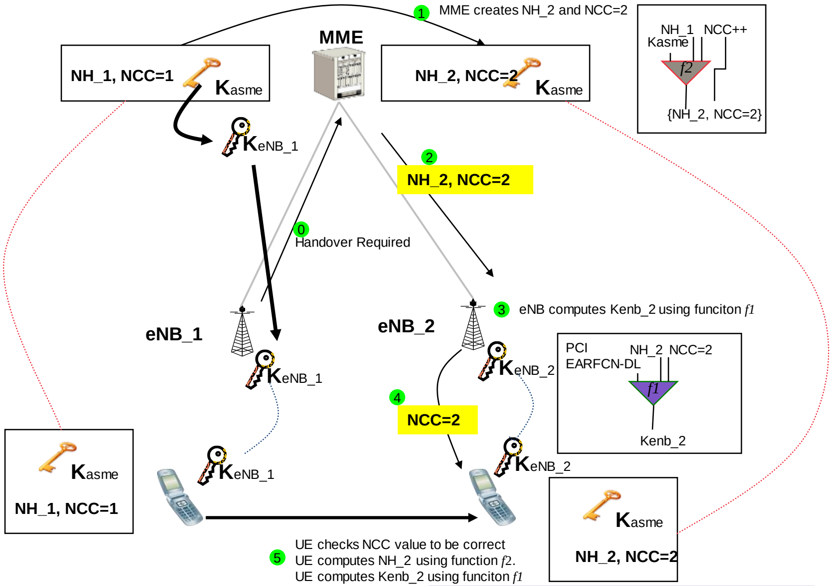


5 UE checks NCC value to be correct
UE computes NH_2 using function *f2*.
UE computes Kenb_2 using funciton *f1*

PCI:	Physical Cell Identity
EARFCN-DL:	E-UTRAN Absolute Frequency Channel –DL
NH	Next Hop Parameter
NCC	NH Chaining Counter

104

Kenb Key Derivation at S1 Handover



1 MME creates NH_2 and NCC=2

2 NH_2, NCC=2

0 Handover Required

3 eNB computes Kenb_2 using funciton *f1*

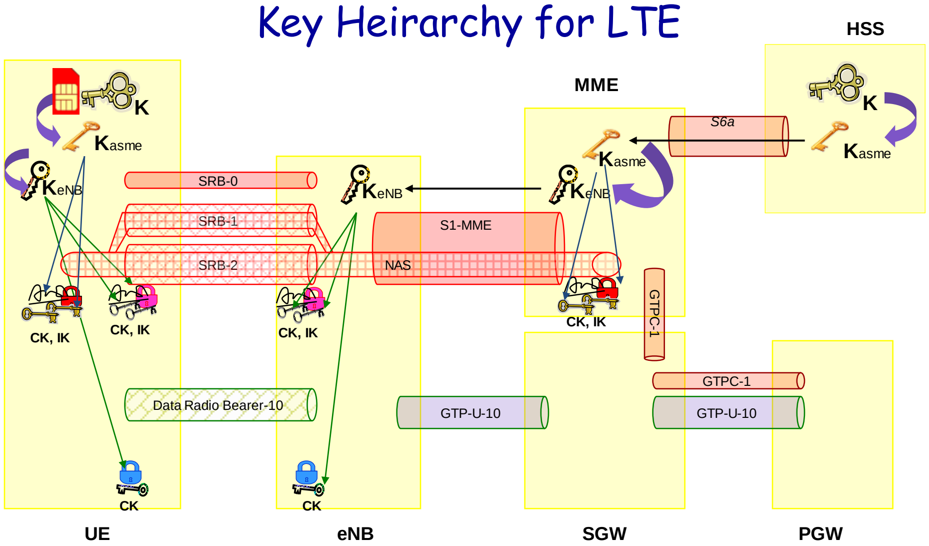
4 NCC=2

5 UE checks NCC value to be correct
UE computes NH_2 using function *f2*.
UE computes Kenb_2 using funciton *f1*

PCI:	Physical Cell Identity
EARFCN-DL:	E-UTRAN Absolute Frequency Channel –DL
NH	Next Hop Parameter
NCC	NH Chaining Counter

105

Key Heirarchy for LTE



▦ Encrypted Info
▨ Integrity Protected Info

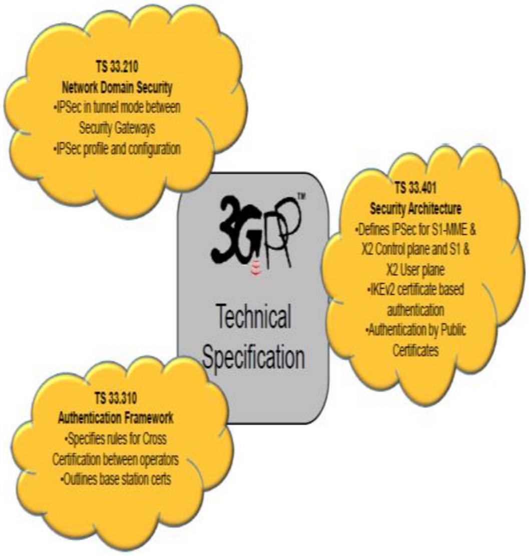
ASME	Access Security Management Entity (MME)
CK, IK	Ciphering Key, Integrity Protection Key

106

Summary

- Authentication in GSM
  - Challenge response based
  - One-way
  - Long term key
- Authentication in LTE (EPS)
  - Challenge-response based
  - Mutual authentication
  - Hierarchical involving many NW nodes (HSS, MME, and eNB)
  - Dynamic key derivation

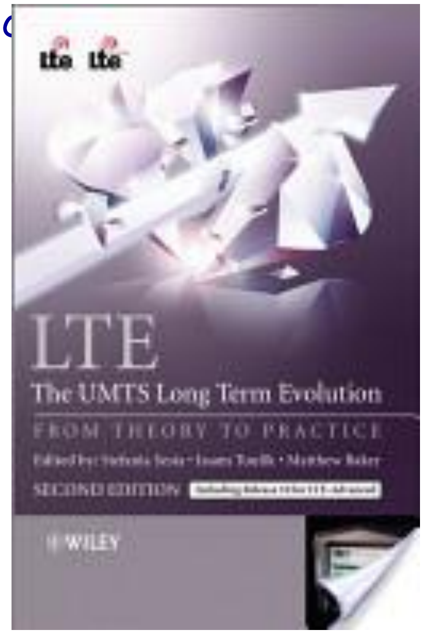
Referenc



TS 33.210
Network Domain Security
•IPSec in tunnel mode between Security Gateways
•IPSec profile and configuration

TS 33.401
Security Architecture
•Defines IPSec for S1-MME & X2 Control plane and S1 & X2 User plane
•IKEv2 certificate based authentication
•Authentication by Public Certificates

TS 33.310
Authentication Framework
•Specifies rules for Cross Certification between operators
•Outlines base station certs



lte lte
LTE
The UMTS Long Term Evolution
FROM THEORY TO PRACTICE
Edited by Stefania Sesia • Issam Toufik • Matthew Baker
SECOND EDITION
WILEY

Specifications

- TS 33.401 – LTE Security
- TS 33.102 – 3G Security

Summary – Part I

- **Migration scenarios from legacy NWs to EPS**
- **LTE Requirements & History**
- **EPS Architecture, Components, and Protocols**